TINA WOLFSON (SBN 174806)
twolfson@ahdootwolfson.com
ROBERT AHDOOT (SBN 172098)
rahdoot@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310.474.9111
Facsimile: 310.474.8585

ANDREW W. FERICH (admitted *pro hac vice*)
aferich@ahdootwolfson.com
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585

BEN BARNOW (admitted *pro hac vice*)
b.barnow@barnowlaw.com
ANTHONY L. PARKHILL (admitted *pro hac vice*)
aparkhill@barnowlaw.com
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Suite 1630
Chicago, IL 60606
Telephone: 312.621.2000

Attorneys for Plaintiffs and the Proposed Class

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

DOUGLAS FEHLEN, TONY BLAKE, DAVID ARTUSO, TERESA BAZAN, LORRIEL CHHAY, SAMANTHA GRIFFITH, ALLEN CHAO, and AUGUSTA MCCAIN, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

ACCELLION, INC.,

Defendant.

Case No. 5:21-cv-01353-EJD

Hon. Edward J. Davila

SECOND AMENDED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Complaint Filed March 17, 2021

Plaintiffs Douglas Fehlen, Tony Blake, David Artuso, Teresa Bazan, Lorriel Chhay, Samantha Griffith, Allen Chao, and Augusta McCain ("Plaintiffs"), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to themselves, respectively, and on information and belief as to all other matters, by and through undersigned counsel, bring this Second Amended Class Action Complaint against Defendant Accellion, Inc. ("Accellion" or "Defendant").

NATURE OF THE ACTION

1. Plaintiffs bring this class action on behalf of themselves and all other individuals ("Class Members") who had their sensitive personal information—i.e., information that is or could be used, whether on its own or in combination with other information, to identify, locate, or contact a person, including without limitation names, email addresses, phone numbers, home addresses, dates of birth, Social Security numbers ("SSN"), drivers' license information, tax records, bank account and routing information, and other personally identifying information, as well as information used to process health insurance claims, prescription information, medical records and data, and other personal health information ("Personal Information")—disclosed to unauthorized third parties during a data breach compromising Accellion's legacy File Transfer Appliance software and divulging sensitive Personal Information of the customers and other affiliates of Accellion's file transfer clients who use(d) the File Transfer Appliance (the "Data Breach" or "Attacks").

2. Accellion made headlines in late 2020/early 2021 (and continues to receive a raft of negative publicity) following its December 23, 2020 disclosure to numerous clients that criminals breached Accellion's client submitted data via a vulnerability in its represented "secure" file transfer application.[1]

3. Accellion is a software company that provides third-party file transfer services to clients. Accellion makes and sells a file transfer service product called the File Transfer Appliance ("FTA").

[1] Lucas Ropek, *The Accellion Data Breach Seems to Be Getting Bigger,* GIZMODO (Feb. 11, 2021, 8:47 P.M.), https://gizmodo.com/the-accellion-data-breach-seems-to-be-getting-bigger-1846250357.

Accellion's FTA is a 20-year-old, obsolete, "legacy" product that was "nearing end-of-life"[2] at the time of the Data Breach, thus leaving it vulnerable to compromise and security incidents.

4. During the Data Breach, unauthorized persons gained access to Accellion's clients' files by exploiting a vulnerability in Accellion's FTA platform.

5. The Kroger Co. ("Kroger") is an Accellion file transfer software client that used the FTA. On or about February 19, 2021, Kroger publicly confirmed that the Personal Information of Kroger pharmacy customers, along with "certain associates' HR data . . . and certain money services records," may have been compromised in the Accellion FTA Data Breach.

6. Flagstar Bank ("Flagstar") is an Accellion file transfer software client that used the FTA. On or about March 5, 2021, Flagstar publicly confirmed that the Personal Information of certain customers and other persons may have been compromised in the Accellion FTA Data Breach.

7. Centene Corporation and various of its health-services-related entities including Health Net (collectively, "Health Net") are Accellion file transfer software clients that used the FTA. On or about March 24, 2021, Health Net publicly confirmed that the Personal Information of certain customers may have been compromised in the Accellion FTA Data Breach.

8. The Office of the Washington State Auditor is an Accellion file transfer software client that used the FTA. In or about the week of February 1, 2021, the Washington State Auditor's office confirmed that the Personal Information of certain persons, including individuals who filed claims with Washington state for unemployment benefits, may have been compromised in the Accellion FTA Data Breach.

9. The Regents of the University of California ("UC") is an Accellion file transfer software client that used the FTA. In or about May 2021, UC confirmed that the Personal Information of certain members of the UC community may have been compromised in the Accellion FTA Data Breach.

[2] ACCELLION, *Accellion Provides Update to Recent FTA Security Incident* (Feb. 1, 2021), https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/.

10. The University of Colorado is an Accellion file transfer software client that used the FTA. In early 2021, the University of Colorado confirmed that the Personal Information of certain members of the University of Colorado community may have been compromised in the Accellion FTA Data Breach.

11. Public reports have revealed that Kroger's, Flagstar's, Health Net's, the Washington State Auditor's, the UC's, the University of Colorado's, and numerous other impacted FTA clients' (altogether, the "Impacted Clients") files containing sensitive Personal Information were impacted by the FTA Data Breach. Accellion has notified numerous of Impacted Clients that an unauthorized person or unauthorized persons gained access to certain clients' files by exploiting vulnerabilities in Accellion's FTA platform.

12. Accellion's services to its clients, and the other customers, included the use of Accellion's outdated and vulnerable FTA platform for large file transfers. The Personal Information of the customers of (and others affiliated with) Accellion's Impacted Clients was accessed by and disclosed to criminals without authorization because the criminals were able to exploit the vulnerabilities in the FTA product.

13. Accellion was well aware of the data security shortcomings in its FTA product. Nevertheless, Accellion continued to use FTA with its clients, putting its file transfer service clients and their clients' customers, employees, and other affiliated persons at risk of being impacted by a breach.

14. Accellion's failure to ensure that its file transfer services and products were adequately secure fell far short of its obligations and Plaintiffs' and Class Members' reasonable expectations for data privacy, has jeopardized the security of their Personal Information, and has put them at serious and a continuing risk of fraud and identity theft.

15. As a result of Accellion's conduct and the Data Breach, Plaintiffs' and Class Members' privacy has been invaded. Their Personal Information is now in the hands of criminals, and they face a substantially increased risk of identity theft and fraud. Accordingly, these individuals now must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

PARTIES

16. Plaintiff Douglas Fehlen is a citizen of Washington and resides in Vancouver, Washington. Plaintiff Fehlen received a notice letter from Kroger stating that his sensitive Personal Information was compromised by the Data Breach. In the letter, Kroger confirmed to Plaintiff that "[this] incident involved your personal information" and that the "impacted information may include names, email address and

other contact information, date of birth, Social Security number, and for some associates or former associates, may have also included certain salary information . . . ."

17. Plaintiff Tony Blake is a citizen of North Carolina and resides in Chapel Hill, North Carolina. Plaintiff Blake received a notice letter from Kroger stating that his sensitive Personal Information was compromised by the Data Breach. In the letter, Kroger confirmed to Plaintiff that "[this] incident involved your personal information" and that the "[i]mpacted information includes all, or a subset of, the following: certain names, email address, phone numbers, home addresses, dates of birth, information to process insurance claims, prescription information such as prescription number, prescribing doctor, medication names and dates, medical history, as well as certain clinical services, such as whether you were ordered an influenza test."

18. Plaintiff David Artuso is a citizen of the state of California and resides in Carmarillo, California. Plaintiff Artuso received a letter from Flagstar confirming that his sensitive Personal Information was compromised by the Data Breach. In the letter, Flagstar identified that the nature of the information compromised includes "your Social Security Number, First Name, Last Name, Phone Number, Address."

19. Plaintiff Teresa Bazan is a citizen of the state of California and resides in Gardenas, California. Plaintiff Bazan received a letter from Health Net confirming that her sensitive Personal Information was compromised by the Data Breach. In the letter, Health Net identified that the nature of the information compromised includes Plaintiff's "Address; Date of Birth; Insurance ID Number; Health information, such as your medical condition(s) and treatment information."

20. Plaintiff Samantha Griffith is a citizen of the state of Washington and resides in Vancouver, Washington. Plaintiff Griffith received an e-mail from the Washington State Auditor's office confirming that her sensitive Personal Information was compromised by the Data Breach. In the e-mail, the Washington State Auditor's office identified that the nature of the information compromised includes "personal information of people who received unemployment benefits from the State of Washington in the 2017 to 2020 time period."

21. Plaintiff Lorriel Chhay is a citizen of the state of Washington and resides in Vancouver, Washington. Plaintiff Chhay received an e-mail from the Washington State Auditor's office confirming

that his sensitive Personal Information was compromised by the Data Breach. In the e-mail, the Washington State Auditor's office identified that the nature of the information compromised includes "personal information of people who received unemployment benefits from the State of Washington in the 2017 to 2020 time period."

22. Plaintiff Allen Chao is a citizen of the state of California and resides in Irvine, California. Plaintiff Chao received an e-mail from UC confirming that his sensitive Personal Information may have been compromised by the Data Breach. In the letter, UC identified that the nature of the information compromised includes "full names, addresses, telephone numbers, Social Security numbers, driver's license information, passport information, financial information including bank routing and account numbers, health and related benefit information, disability information and birthdates, as well as other personal information. The impacted information also includes your response to the 2020 UC Undergraduate Experience Survey."

23. Plaintiff Augusta McCain is a citizen of the state of California and resides in La Mesa, California. Plaintiff McCain received an e-mail from the University of Colorado confirming that her sensitive Personal Information may have been compromised by the Data Breach. In the letter, the University of Colorado identified that the nature of the information compromised includes "your name in combination with: Date of Birth, Student Demographic Information, Course Information, Student Financial Information, and Student ID."

24. Defendant Accellion Inc. is a Delaware corporation with corporate headquarters located at 1804 Embarcadero Road, Suite 200, Palo Alto, California 94303.

JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00) and is a class action in which Plaintiffs are citizens of states different from Defendant. Further, greater than two-thirds of the Class Members reside in states other than the state in which Defendant is a citizen.

26. The Court has personal jurisdiction over Accellion because Accellion has a principal office in California, does significant business in California, and otherwise has sufficient minimum contacts with

and intentionally avails itself of the markets in California through its promotion, marketing, and sale of file transfer services.

27. Venue properly lies in this judicial district because, *inter alia,* Defendant has a principal place of business, transacts substantial business, has agents, and is otherwise located in this district; and a substantial part of the conduct giving rise to the claims occurred in this judicial district.

FACTUAL ALLEGATIONS

A. Accellion and its Unsecure File Transfer Platform, FTA

28. Accellion is a Palo Alto-based software company that makes, markets, and sells file transfer platforms and services.

29. Accellion touts its products and services as "prevent[ing] data breaches"[3] and as being secure. On its website, Accellion states:

> The Accellion enterprise content firewall *prevents data breaches and compliance violations from third party cyber risk*. CIOs and CISOs *rely on the Accellion platform for complete visibility, security and control* over . . . *sensitive content* across email, file sharing, mobile, enterprise apps, web portals, SFTP, and automated inter-business workflows.[4]

30. Accellion also touts its commitment to data privacy, claiming that "[d]ata privacy is a fundamental aspect of the business of Accellion . . . ."[5]

31. Accellion markets its products and services as capable of safely transferring sensitive information through file sharing, claiming that "[w]hen employees click the Accellion button, they know it's the *safe*, *secure* way to share sensitive information. . . ."[6]

32. Despite these assurances and claims, Accellion failed to offer safe and secure file transfer products and services and failed to adequately protect Plaintiffs' and Class Members' Personal Information entrusted to it by Accellion's clients.

---

[3] ACCELLION, *About Accellion,* https://www.accellion.com/company/ (last visited Dec. 9, 2021).

[4] *Id.* (emphasis added).

[5] ACCELLION, *Accellion Privacy Policy*, https://www.accellion.com/privacy-policy/ (last visited Dec. 9, 2021).

[6] ACCELLION, *About Accellion*, https://www.accellion.com/company/ (emphasis added) (last visited Dec. 9, 2021).

33. This is because the product that Accellion offered, and which its clients used, was not secure and, by Accellion's own acknowledgment, outdated.

34. The FTA—or File Transfer Appliance—is Accellion's twenty-year-old "legacy" file transfer software, which purportedly is designed and sold for large file transfers.[7]

35. According to Accellion, the product has become an obsolete "legacy product" that was "nearing end-of-life,"[8] thus leaving it vulnerable to compromise and security incidents. Accellion acknowledged that the FTA program is insufficient to keep file transfer processes secure "in today's breach-filled, over-regulated world" where "you need even broad protection and control."[9]

36. Key people within Accellion have acknowledged the need to leave the FTA platform behind due to the security concerns raised by it. Accellion's Chief Marketing Officer Joel York confirmed that Accellion is encouraging its clients to discontinue use of FTA because it does not protect against modern data breaches: "It just wasn't designed for these types of threats . . . ."[10]

37. Accellion's Chief Information Security Officer Frank Balonis stated: "Future exploits of [FTA] . . . are a constant threat. We have encouraged all FTA customers to migrate to kiteworks for the last three years and have accelerated our FTA end-of-life plans in light of these attacks. We remain committed to assisting our FTA customers, but strongly urge them to migrate to kiteworks as soon as possible."[11]

38. Despite knowing that FTA leaves Accellion customers and third parties interacting and transacting with its customers (like Plaintiffs and other Class Members) exposed to security threats, it continued to offer and transact business with its customers using the FTA file transfer product.

---

[7] ACCELLION, *Accellion Responds to Recent FTA Security Incident* (Jan. 12, 2021), https://www.accellion.com/company/press-releases/accellion-responds-to-recent-fta-security-incident/.

[8] ACCELLION, *Press Release, Accellion Provides Update to Recent FTA Security Incident*, *supra* note 2.

[9] ACCELLION, *Accellion FTA*, https://www.accellion.com/products/fta/ (last visited Dec. 9, 2021).

[10] Jim Brunner & Paul Roberts, *Banking, Social Security info of more than 1.4 million people exposed in hack involving Washington State Auditor*, SEATTLE TIMES (Feb. 3, 2021, 4:57 P.M.), https://www.seattletimes.com/seattle-news/politics/personal-data-of-1-6-million-washington-unemployment-claimants-exposed-in-hack-of-state-auditor/.

[11] ACCELLION, *Press Release, Accellion Provides Update to Recent FTA Security Incident*, *supra* note 2.

B. The Accellion Data Breach

39. On December 23, 2020, the inevitable happened: Accellion confirmed to numerous clients that it experienced a massive security breach whereby criminals were able to gain access to sensitive client data via a vulnerability in its FTA platform.[12]

40. According to reports, the criminals exploited as many as four vulnerabilities in Accellion's FTA to steal sensitive data files associated with up to 300 of Accellion's clients, including corporations, law firms, banks, universities, and other entities.

41. With respect to how Accellion's FTA was compromised, one report indicates:

> The adversary exploited [the FTA's] vulnerabilities to install a hitherto unseen Web shell named DEWMODE on the Accellion FTA app and used it to exfiltrate data from victim networks. Mandiant's telemetry shows that DEWMODE is designed to extract a list of available files and associated metadata from a MySQL database on Accellion's FTA and then download files from that list via the Web shell. Once the downloads complete, the attackers then execute a clean-up routine to erase traces of their activity.[13]

42. The criminals, reportedly associated with the well-known Clop ransomware gang, the FIN11 threat group, and potentially other threat actors, launched the attacks in mid-December 2020. The attacks continued from at least mid-December 2020 and into January 2021, as these actors continued to exploit vulnerabilities in the FTA platform. Following the attacks, the criminals resorted to extortion, threatening Accellion's clients, e.g., by email, with making the stolen information publicly available unless ransoms were paid.[14] In at least a few instances, the criminals carried these threats and published private and confidential information online.

---

[12] Lucas Ropek, *The Accellion Data Breach Seems to Be Getting Bigger,* GIZMODO (Feb. 11, 2021), https://gizmodo.com/the-accellion-data-breach-seems-to-be-getting-bigger-1846250357.

[13] Jai Vljayan, *Accellion Data Breach Resulted in Extortion Attempts Against Multiple Victims,* DARKREADING (Feb. 22, 2021, 4:50 P.M.), https://www.darkreading.com/attacks-breaches/accellion-data-breach-resulted-in-extortion-attempts-against-multiple-victims/d/d-id/1340226.

[14] Ionut Ilascu, *Global Accellion data breaches linked to Clop ransomware gang,* BLEEPINGCOMPUTER (Feb. 22, 2021, 9:06 A.M.), https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/.

43. An example of a message reportedly sent by the criminals to a client of Accellion that was victimized during the breach is below[15]:

> Hello!
>
> Your network has been hacked, a lot of valuable data stolen. <description of stolen data, including the total size of the compressed files> We are the CLOP ransomware team, you can google news and articles about us. We have a website where we publish news and stolen files from companies that have refused to cooperate. Here is his address http://[redacted].onion/ - use TOR browser or http://[redacted].onion.dog/ - mirror. We are visited by 20-30 thousand journalists, IT experts, hackers and competitors every day. We suggest that you contact us via chat within 24 hours to discuss the current situation. <victim-specific negotiation URL> - use TOR browser We don't want to hurt, our goal is money. We are also ready to provide any evidence of the presence of files with us.

44. Accellion remained in the headlines through early- to mid-2021 following its mid-December 2020 disclosure of the massive Data Breach. The list of groups and clients who used Accellion's unsecure FTA product and were impacted by the Data Breach continues to increase and includes, among others:

- Allens
- American Bureau of Shipping ("ABS")
- Arizona Complete Health
- The Australia Securities and Investments Commission
- Bombardier
- CSX
- Danaher
- Flagstar Bank
- Fugro
- Goodwin Proctor
- Harvard Business School
- Health Net (and other related entities)

[15] *Id.*

- Jones Day
- The Kroger Co.
- The Office of the Washington State Auditor
- QIMR Berghofer Medical Research Institute
- Qualys
- The Reserve Bank of New Zealand
- Shell
- Singtel
- Southern Illinois University School of Medicine
- Stanford University
- Steris
- Transport for New South Wales
- Trillium Community Health Plan
- University of California system
- University of Colorado
- University of Maryland, Baltimore
- University of Miami (Florida)
- Yeshiva University.

C. Impact of the Data Breach

45. As a result of the FTA Data Breach, Plaintiffs and millions of individuals have had their information exposed. Numerous other Accellion clients have reported being impacted by the Data Breach, and potentially millions of additional persons have had their sensitive Personal Information exposed as a result of Accellion's unsecure FTA product being exploited by criminals during the Data Breach.

46. The harm caused to Plaintiffs and Class Members by the Data Breach is already apparent. As identified herein, criminal hacker groups have threatened some of Accellion's Impacted Clients with demands for ransom payments to prevent sensitive information from being disseminated publicly.

47. Even if companies that were impacted by the Data Breach pay these ransoms, there is no guarantee that the criminals making the ransom demands will suddenly act honorably and destroy the sensitive information. In fact, there is no motivation for them to do so, given the burgeoning market for sensitive Personal Information on the dark web.

48. The breach creates a heightened security concern for Plaintiffs and Class Members because SSNs, financial and banking information, and sensitive medical, health, and prescription information was among the data exposed during the Data Breach.

49. Theft of SSNs creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

50. Given the highly sensitive nature of SSNs, theft of SSNs in combination with other personally identifying information (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. Per the United States Attorney General, Social Security numbers "can be an identity thief's most valuable piece of consumer information."[16]

51. Accellion had a duty to keep sensitive information confidential and to protect it from unauthorized disclosures. Plaintiffs and Class Members provided their Personal Information to Kroger, Flagstar, Health Net, the Washington State Auditor, UC, the University of Colorado, and other Impacted Clients with the common sense understanding any business partners to these entities disclosed the Personal Information (i.e., Accellion) would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

52. Accellion's data security obligations were particularly important given the substantial increase in data breaches—particularly those involving SSNs and health information—in recent years, which are widely known to the public and to anyone in Accellion's industry of data collection and transfer.

---

[16] *Fact Sheet: The Work of the President's Identity Theft Task Force*, DEP'T OF JUSTICE, (Sept. 19, 2006), https://www.justice.gov/archive/opa/pr/2006/September/06_ag_636.html.

53. Data breaches are by no means new, and they should not be unexpected. These types of attacks should be anticipated by companies that store sensitive and personally identifying information, and these companies must ensure that data privacy and security is adequate to protect against and prevent known attacks.

54. It is well known among companies that store sensitive personally identifying information that sensitive information—like the SSNs and health information stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers. . . . Many of them were caused by flaws in . . . systems either online or in stores."[17]

55. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, tax fraud, phone or utilities fraud, and bank/finance fraud.

56. There may be a time lag between when sensitive Personal Information is stolen and when it is used. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, *stolen data may be held for up to a year or more before being used to commit identity theft*. Further, once stolen data have been sold or posted on the Web, *fraudulent use of that information may continue for years*. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[18]

57. With access to an individual's sensitive Personal Information, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive

[17] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[18] *Id*. at 29 (emphasis added).

medical services in the victim's name, and may even give the victim's Personal Information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[19]

58. Sensitive Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web and the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen SSNs and other sensitive Personal Information directly on various illegal websites making the information publicly available, often for a price.

59. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[20] Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

60. Medical information is especially valuable to identity thieves. According to a 2012 Nationwide Insurance report, "[a] stolen medical identity has a $50 street value . . . ."[21] In fact, the medical industry has experienced disproportionally higher instances of computer theft than any other industry.

61. Despite the known risk of data breaches and the widespread publicity and industry alerts regarding other notable (similar) data breaches, Accellion failed to take reasonable steps to adequately protect its systems from being breached and to properly phase out its unsecure FTA platform, which it knew was unsecure, leaving its clients (including the Impacted Clients) and all persons who provide sensitive Personal Information to those clients (i.e., Plaintiffs and the Class Members) exposed to risk of fraud and identity theft.

62. Accellion is, and at all relevant times has been, aware that the sensitive Personal Information it handles and stores in connection with providing its file transfer services is highly sensitive.

---

[19] *See* FEDERAL TRADE COMMISSION, WARNING SIGNS OF IDENTITY THEFT, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited Feb. 22, 2021).

[20] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010, 5:00 A.M.), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.

[21] Study: Few Aware of Medical Identity Theft Risk, CLAIMS JOURNAL (June 14, 2012), http://www.claimsjournal.com/news/national/2012/06/14/208510.htm.

As a company that provides file transfer services involving highly sensitive and identifying information, Accellion is aware of the importance of safeguarding that information and protecting its systems and products from security vulnerabilities.

63. Accellion was aware, or should have been aware, of regulatory and industry guidance regarding data security, and it was alerted to the risk associated with failing to ensure that its file transfer product FTA was adequately secured, or phasing out the platform altogether.

64. Despite the well-known risks of hackers, cybercriminals, data breaches, and cybersecurity intrusions, Accellion failed to employ adequate data security measures in connection with offering its FTA file transfer product and related services in a meaningful way in order prevent breaches, including the Data Breach.

65. The security flaws inherent to Accellion's FTA file transfer platform—and continuing to market and sell a platform with known, unpatched security issues—run afoul of industry best practices and standards. Had Accellion adequately protected and secured FTA, or stopped supporting the product when it learned years ago about its vulnerabilities, it could have prevented the Data Breach.

66. Despite the fact that Accellion was on notice of the very real possibility of data theft associated with the FTA platform, it still failed to make necessary changes to the product or to stop offering and supporting it, and permitted a massive intrusion to occur that resulted in the FTA platform's disclosure of Plaintiffs' and Class Members' Personal Information to criminals.

67. Accellion permitted Class Members' Personal Information to be compromised and disclosed to criminals by failing to take reasonable steps against an obvious threat.

68. Industry experts are clear that a data breach is indicative of data security failures. Indeed, industry-leading research and advisory firm Aite Group has identified that: "If your data was stolen through a data breach that means you were somewhere out of compliance" with payment industry data security standards.[22]

[22] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 26, 2017), http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY.

69. As a result of the events detailed herein, Plaintiffs and Class Members suffered harm and loss of privacy, and will continue to suffer future harm, resulting from the Data Breach, including but not limited to: invasion of privacy; loss of privacy; loss of control over personal information and identities; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value and loss of possession and privacy of Personal Information; harm resulting from damaged credit scores and information; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized exposure of Personal Information.

70. Victims of the Data Breach have likely already experienced harms, which is made clear by news of attempts to exploit this information for money by the hackers responsible for the breach.

71. As a result of Accellion's failure to ensure that its FTA product was protected and secured, or to phase out the platform upon learning of FTA's vulnerabilities, the Data Breach occurred. As a result of the Data Breach, Plaintiffs' and Class Members' privacy has been invaded, their Personal Information is now in the hands of criminals, they face a substantially increased risk of identity theft and fraud, and they must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

CLASS ALLEGATIONS

72. Plaintiffs bring this action on their own behalf, and on behalf of the following Class:

> All natural persons who are residents of the United States whose Personal Information was stored on the FTA systems of FTA Customers and was compromised in the Attacks, including all natural persons who are residents of the United States who were sent notice by an FTA Customer that their Personal Information may have been compromised in the Attacks.

73. Excluded from the Class are: are: (1) the Judges presiding over the Action and members of their families; (2) Accellion, its subsidiaries, parent companies, successors, predecessors, and any entity in which Accellion or its parents, have a controlling interest, and its current or former officers and directors; (3) natural persons who properly execute and submit a Request for Exclusion prior to the expiration of the Opt-Out Period; and (4) the successors or assigns of any such excluded natural person.

74. **Numerosity**: While the precise number of Class Members has not yet been determined, members of the Class are so numerous that their individual joinder is impracticable, as the proposed Class appears to include many millions of members who are geographically dispersed.

75. **Typicality**: Plaintiffs and all Class Members were injured through Accellion's uniform misconduct and assert similar claims against Accellion. Accordingly, Plaintiffs' claims are typical of Class Members' claims.

76. **Adequacy**: Plaintiffs' interests are aligned with the Class they seek to represent and they have retained counsel with significant experience prosecuting complex class action cases, including cases involving privacy and data security violations. Plaintiffs and counsel intend to prosecute this action vigorously. The Class's interests are well-represented by Plaintiffs and undersigned counsel.

77. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiffs' and other Class Member's claims. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class Members individually to effectively redress Accellion's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

78. **Commonality and Predominance:** The following questions common to all Class Members predominate over any potential questions affecting individual Class Members:

- whether Accellion engaged in the wrongful conduct alleged herein;
- whether Accellion was negligent or negligent per se;
- whether Accellion's data security practices and the vulnerabilities of its FTA product resulted in the unauthorized disclosure of Plaintiffs' and other Class Members' Personal Information;
- whether Accellion violated privacy rights and invaded Plaintiffs' and Class Members'

privacy; and

- whether Plaintiffs and Class Members are entitled to damages, equitable relief, or other relief and, if so, in what amount.

79. Given that Accellion has engaged in a common course of conduct as to Plaintiffs and the Class, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

80. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

81. Accellion negligently sold and continued to support its unsecure FTA product which it has acknowledged was vulnerable to security breaches, despite representing that the product could be used securely for large file transfers.

82. Accellion was entrusted with, stored, and otherwise had access to the Personal Information of Plaintiffs and Class Members.

83. Accellion knew, or should have known, of the risks inherent to storing the Personal Information of Plaintiffs and Class Members, and to not ensuring that the FTA product was secure. These risks were reasonably foreseeable to Accellion, including because it had previously recognized and acknowledged the data security concerns with its FTA product.

84. Accellion owed duties of care to Plaintiffs and Class Members whose Personal Information had been entrusted to Accellion.

85. Accellion breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate data security. Accellion had a duty to safeguard Plaintiffs' and Class Members' Personal Information and to ensure that its systems and products adequately protected Personal Information. Accellion breached its duty.

86. Accellion's duty of care arises from its knowledge that its file transfer customers entrust to it highly sensitive Personal Information that Accellion is intended to, and represents that it will, handle securely. Only Accellion was in a position to ensure that its systems and products were sufficient to protect

against breaches that exploit its FTA product and the harms that Plaintiffs and Class Members have now suffered.

87. A "special relationship" exists between Accellion, on the one hand, and Plaintiffs and Class Members, on the other hand. Accellion entered into a "special relationship" with Plaintiffs and Class Members by agreeing to accept, store, and have access to sensitive Personal Information provided by Plaintiffs and Class Members to Accellion's clients.

88. But for Accellion's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

89. Accellion acted with wanton disregard for the security of Plaintiffs' and Class Members' Personal Information, especially in light of the fact that for years Accellion warned of the data security concerns relating to the FTA.

90. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Accellion's breach of its duties. Accellion knew or should have known that it was failing to meet its duties, and that Accellion's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Personal Information.

91. Plaintiffs and Class Members suffered more than just economic harm as a result of the Data Breach. Plaintiffs and Class Members suffered loss of time, loss of value of their Personal Information, and loss of privacy concerning their Personal Information.

92. As a direct and proximate result of Accellion's negligent conduct, Plaintiffs and Class Members now face a certain increased risk of future harm. For them, the purpose for criminals to steal Personal Information is to sell it on the dark web for a profit to other criminals who purchase the information and use it to make fraudulent transactions or to support ransomware.

93. As a direct and proximate result of Accellion's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence Per Se
(On Behalf of Plaintiffs and the Class)

94. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

95. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Accellion had a duty to provide adequate data security practices, including in connection with its sale of its FTA platform, to safeguard Plaintiffs' and Class Members' Personal Information.

96. Pursuant to HIPAA (42 U.S.C. §§ 1302d, *et seq*.), Accellion had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Personal Information.

97. Accellion breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45) and HIPAA (42 U.S.C. §§ 1302d, *et. seq*.), among other laws, by failing to provide fair, reasonable, or adequate data security in connection with the sale and use of the FTA platform in order to safeguard their Personal Information.

98. Accellion's failure to comply with applicable laws and regulations constitutes negligence per se.

99. But for Accellion's wrongful and negligent breach of its duties owed to Plaintiffs and other Class Members, they would not have been injured.

100. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Accellion's breach of its duties. Accellion knew or should have known that it was failing to meet its duties, and that Accellion's breach would cause Plaintiffs and other Class Members to experience the foreseeable harms associated with the exposure of their Personal Information.

101. As a direct and proximate result of Accellion's negligent conduct, Plaintiffs and other Class Members have suffered loss of time, loss of value of their Personal Information, and loss of privacy concerning their Personal Information, and now face an increased risk of future harm. As a direct and proximate result of Accellion's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
Invasion of Privacy (Intrusion Upon Seclusion)
(On Behalf of Plaintiffs and the Class)

102. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

103. Plaintiffs and other Class Members had a reasonable expectation of privacy in the Personal Information that Accellion disclosed without authorization.

104. By failing to keep Plaintiffs' and other Class Members' Personal Information safe,

knowingly utilizing and continuing support for the unsecure FTA platform, and disclosing Personal Information to unauthorized parties for unauthorized use, Accellion unlawfully invaded Plaintiffs' and Class Members' privacy by, *inter alia*:

(a) intruding into Plaintiffs' and Class Members' private affairs in a manner that would be highly offensive to a reasonable person; and

(b) invading Plaintiffs' and Class Members' privacy by improperly using their Personal Information properly obtained for a specific purpose for another purpose, or disclosing it to some third party;

(c) failing to adequately secure their Personal Information from disclosure to unauthorized persons; and

(d) enabling the disclosure of Plaintiffs' and Class Members' Personal Information without consent.

105. Accellion knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' and Class Members' position would consider its actions highly offensive.

106. Accellion knew that its FTA platform was vulnerable to exploitation and a breach prior to the Data Breach.

107. Defendant invaded Plaintiffs' and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private affairs by disclosing their Personal Information to unauthorized persons without their informed, voluntary, affirmative, and clear consent.

108. As a proximate result of such unauthorized disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their Personal Information was unduly frustrated and thwarted. Defendant's conduct amounted to a serious invasion of Plaintiffs' and Class Members' protected privacy interests.

109. In failing to protect Plaintiffs' and Class Members' Personal Information, and in disclosing Plaintiffs' and Class Members' Personal Information, Accellion acted with malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private.

110. Plaintiffs seek injunctive relief on behalf of the Class, restitution, and all other damages available under this Count.

COUNT IV
Violation of the North Carolina Unfair and Deceptive Trade Practices Act
N.C. Gen. Stat. §§ 75-1.1 *et seq.* ("NC UDTPA")
(On Behalf of Plaintiff Blake and the Class)

111. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

112. N.C. Gen. Stat. § 75-1.1(a) states: "Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are declared unlawful."

113. Defendant's failure to disclose that its data privacy measures are inadequate to protect Class Member Personal Information, and its continued use and support of the FTA platform with file transfer clients—who entrusted Accellion with Class Members' sensitive Personal Information—despite knowing that the FTA was unsecure and vulnerable to exploitation and data breaches, constitutes an unfair practice in violation of N.C. Gen. Stat. Ann. § 75-1.1.

114. Plaintiff Blake and Class Members in North Carolina are persons who provided their Personal Information to Accellion's Impacted Clients, who in turn entrusted that sensitive information to Accellion in connection with file transfer activities.

115. Accellion knew for years that its FTA was unsecure, including at the time Plaintiff Blake and Class Members' Personal Information was entrusted to Accellion. In fact, Accellion had been encouraging file transfer clients for years to switch to its more secure product, Kiteworks.

116. Accellion's continued use and refusal to end support for the FTA in the face of a real security threat and risk of a data breach, all of which was reasonably foreseeable, constitutes unfair practices in violation of the NC UDTPA.

117. Accellion's practices offend public policy, are immoral, unethical, oppressive, and unscrupulous, and caused substantial injury to consumers.

118. Accellion's unfair acts or practices were the foreseeable and actual cause of Plaintiff Blake and Class Members suffering actual damages.

119. Plaintiff Blake and Class Members suffered ascertainable loss as a direct and proximate result of Accellion's unfair acts or practices. Among other injuries, Plaintiff Blake and Class Members lost time and the privacy and value of their Personal Information.

COUNT V
Violations of the Washington Consumer Protection Act
Wash. Rev. Code § 19.86.010, *et seq.* ("WCPA")
(On Behalf of Plaintiffs Fehlen, Griffith, and Chhay, and the Class)

120. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

121. Accellion and Plaintiffs Fehlen, Griffith, and Chhay are "persons" under Wash. Rev. Code § 19.86.010(1).

122. Accellion's acts or practices, as set forth above, occurred in the conduct of "trade" or "commerce" within the meaning of Wash. Rev. Code § 19.86.010(2).

123. Washington law prohibits "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or practices." Wash. Rev. Code §§ 19.86.020.

124. Accellion's failure to disclose that its data privacy measures are inadequate to protect Class Member Personal Information, and its continued use and support of the FTA platform with file transfer clients—who entrusted Accellion with sensitive Personal Information—despite knowing that the FTA was unsecure and vulnerable to exploitation and data breaches, constitutes an unfair practice in violation of the WCPA.

125. Plaintiffs Fehlen, Griffith, and Chhay, and Class Members in Washington, are persons who provided their Personal Information to Accellion's Impacted Clients, who in turn entrusted that sensitive information to Accellion in connection with file transfer activities.

126. Accellion knew for years that its FTA was unsecure, including at the time Plaintiffs and Class Members' Personal Information was entrusted to Accellion. In fact, Accellion had been encouraging file transfer clients for years to switch to its more secure product, Kiteworks.

127. Accellion's continued use and refusal to end support for the FTA in the face of a real security threat and risk of a data breach, all of which was reasonably foreseeable, constitutes unfair practices in violation of the WCPA.

128. Accellion's practices offend public policy, are immoral, unethical, oppressive, and unscrupulous, and caused substantial injury to consumers.

129. Accellion's unfair acts or practices were the foreseeable and actual cause of Plaintiffs and Class Members suffering actual damages.

130. Plaintiffs Fehlen, Chhay, and Griffith, and Class Members suffered ascertainable loss as a direct and proximate result of Accellion's unfair acts or practices. Among other injuries, Plaintiffs and Class Members lost time and the privacy and value of their Personal Information.

131. Accellion's violations of the WCPA present a continuing risk to Plaintiffs and Class Members, as well as to the general public. Accellion's unlawful acts and practices adversely affect the public interest.

132. Under Wash. Rev. Code § 19.86.090, Plaintiffs seek an order enjoining Accellion's unfair acts or practices, providing for appropriate monetary relief, including trebled damages, and awarding reasonable attorneys' fees and costs.

133. In accordance with Wash. Rev. Code § 19.86.095, a copy of Plaintiffs' previous First Amended Class Action Complaint was served on the Attorney General of Washington.

COUNT VI
Violations of California's Consumer Privacy Act
Cal. Civ. Code § 1798.100, *et seq.* ("CCPA")
(On Behalf of Plaintiffs Artuso, Bazan, Chao, and McCain, and the Class)

134. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

135. The CCPA was enacted to protect consumers' sensitive information from collection and use by businesses without appropriate notice and consent.

136. Through the conduct complained of herein, Accellion violated the CCPA by subjecting the Personal Information of Plaintiffs and Class Members located in California to unauthorized access and exfiltration, theft, or disclosure as a result of Accellion's violation of their duties to implement and maintain reasonable security procedures and practices appropriate to the nature and protection of that information. Cal. Civ. Code § 1798.150(a).

137. In accordance with Cal. Civ. Code §1798.150(b), on July 14, 2021, Plaintiffs' counsel sent Accellion a cure notice of its CCPA violations by certified mail, return receipt requested.

138. Accellion failed to rectify the violations detailed herein, individually and on behalf of California class members. Accordingly, Plaintiffs seek actual, punitive, and statutory damages, restitution, and injunctive relief, and any other relief the Court deems proper, as a result of Accellion's CCPA violations.

COUNT VII
Violation of the California Confidentiality of Medical Information Act
Cal. Civ. Code §§ 56, *et seq.* ("CMIA")
(On Behalf of Plaintiff Bazan and the Class)

139. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

140. Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization[.]"

141. Accellion is a "contractor" within the meaning of Cal. Civ. Code § 56.05(d) and/or a "business organized for the purpose of maintaining medical information" and/or a "business that offers software or hardware to consumers . . . that is designed to maintain medical information" within the meaning of Cal. Civ. Code § 56.06(a) and (b), and maintained and continues to maintain "medical information," within the meaning of Civil Code § 56.05(j), for "patients," within the meaning of Cal. Civ. Code § 56.05(k).

142. Plaintiff and impacted Class Members in California are "patients" within the meaning of Cal. Civ. Code § 56.05(k) and are "endanger[ed]" within the meaning of Cal. Civ. Code § 56.05(e), because Plaintiffs and Class Members fear that disclosure of their Personal Information, including their Personal Health Information ("PHI"), could subject them to harassment or abuse.

143. Plaintiff and impacted Class Members had their Personal Information, including PHI, created, maintained, preserved, and stored on Accellion's computer networks at the time of the Data Breach.

144. Accellion, through inadequate security, allowed an unauthorized third party or third parties to gain access to Plaintiff's and other Class Members' Personal Information, including PHI, without the prior written authorization required by Cal. Civ. Code § 56.10 of the CMIA.

145. Accellion violated Cal. Civil Code § 56.101 of the CMIA by failing to maintain and preserve the confidentiality of Plaintiff's and other Class Members' Personal Information, including PHI.

146. As a result of Accellion's above-described conduct, Plaintiff and Class Members have suffered damages from the unauthorized disclosure and release of their Personal Information, including PHI.

147. As a direct and proximate result of Accellion's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their confidential Personal Information, including PHI and sensitive medical information, (iv) statutory damages under the CMIA, (v) deprivation of the value of their Personal Information, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

148. Plaintiff, individually and for each impacted Class Member, seeks nominal damages of one thousand dollars ($1,000) for each violation under Cal. Civ. Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Cal. Civ. Code § 56.36(b)(2), injunctive relief, as well as punitive damages of up to $3,000 per Plaintiff and impacted Class Member, and attorneys' fees, litigation expenses and court costs, pursuant to Civil Code § 56.35.

COUNT VIII
Violations of the California Customer Records Act
Cal. Civ. Code §§ 1798.80, *et seq.* ("CCRA")
(On Behalf of Plaintiffs Artuso, Bazan, Chao, and McCain, and the Class)

149. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

150. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Civil Code § 1798.81.5, which requires that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security

procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

151. By failing to implement reasonable measures to protect Plaintiffs' and Class Members' Personal Information, Accellion violated Civil Code § 1798.81.5.

152. In addition, by failing to promptly notify all affected Class Members that their Personal Information had been exposed, Accellion violated Civil Code § 1798.82.

153. As a direct or proximate result of Accellion's violations of Civil Code §§ 1798.81.5 and 1798.82, Plaintiffs and Class Members in California were (and continue to be) injured and have suffered (and will continue to suffer) the damages and harms described herein.

154. In addition, by violating Civil Code §§ 1798.81.5 and 1798.82, Accellion "may be enjoined" under Civil Code Section 1798.84(e).

155. Accellion's violations of Civil Code §§ 1798.81.5 and 1798.82 also constitute unlawful acts or practices under the UCL, which affords the Court discretion to enter whatever orders may be necessary to prevent future unlawful acts or practices.

156. Plaintiffs accordingly request that the Court enter an injunction requiring Accellion to implement and maintain reasonable security procedures, including, but not limited to: (1) ordering that Accellion cease support of the FTA platform; (2) ordering that Accellion utilize strong industry standard data security measures and file transfer software for the transfer and storage of customer data; (3) ordering that Accellion, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Accellion's systems on a periodic basis; (4) ordering that Accellion engage third party security auditors and internal personnel to run automated security monitoring; (5) ordering that Accellion audit, test, and train security personnel regarding any new or modified procedures; (6) ordering that Accellion purge, delete, and destroy in a reasonably secure manner Class Member data not necessary for its provisions of services; (7) ordering that Accellion, consistent with industry standard practices, conduct regular database scanning and security checks; (8) ordering that Accellion, consistent with industry standard practices, evaluate all file transfer and other software, systems, or programs utilized for storage and transfer of sensitive Personal Information for vulnerabilities to prevent threats to customers; (9)

ordering that Accellion, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (10) ordering Accellion to meaningfully educate its customers about the threats they face as a result of the loss of their Personal Information to third parties, as well as the steps Accellion's customers must take to protect themselves.

COUNT IX
Violations of the California Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL")
(On Behalf of Plaintiffs and the Class)

157. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

158. Accellion engaged in unfair and unlawful business practices in violation of the UCL.

159. Plaintiffs suffered injury in fact and lost money or property as a result of Accellion's alleged violations of the UCL.

160. The acts, omissions, and conduct of Acellion as alleged constitute a "business practice" within the meaning of the UCL.

Unlawful Prong

161. Accellion violated the unlawful prong of the UCL by violating, without limitation, the CCRA, CCPA, and CMIA, as alleged above.

162. Acccellion's conduct also undermines California public policy—as reflected in statutes like the California Information Practices Act, Cal. Civ. Code §§ 1798, *et seq.*, the CCPA concerning consumer privacy, the CMIA concerning medical records and information, and the CCRA concerning customer records—which seek to protect customer and consumer data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

Unfair Prong

163. Accellion's acts, omissions, and conduct also violate the unfair prong of the UCL because its acts, omissions, and conduct, as alleged herein, offended public policy and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiffs and other Class Members. The gravity of Accellion's conduct outweighs any potential benefits attributable

to such conduct and there were reasonably available alternatives to further Accellion's legitimate business interests, other than Accellion's conduct described herein.

164. Accellion's failure to utilize, and to disclose that they do not utilize, industry standard security practices but, instead, utilize the unsecured FTA platform, constitutes an unfair business practice under the UCL. Accellion's conduct is unethical, unscrupulous, and substantially injurious to the Class. While Accellion's competitors have spent the time and money necessary to appropriately safeguard their products, service, and customer information, Accellion has not—to the detriment of its customers and to competition.

Fraudulent Prong

165. By failing to disclose that it does not enlist industry standard security practices and utilized the unsecured FTA platform despite it being a legacy product that was known to be vulnerable, all of which rendered Class members particularly vulnerable to data breaches, Accellion engaged in UCL-violative practices.

166. A reasonable consumer would not have done business with or paid for services from Accellion's Impacted Clients who use(d) the FTA product if they knew the truth about Accellion's security procedures and that the FTA is an unsecured transfer application. By withholding material information about its security practices, Accellion was able to obtain and retain file transfer customers who used the FTA and to whom Plaintiffs and Class Members provided and entrusted their Personal Information in connection with transacting business with those file transfer clients. Had Plaintiffs known the truth about Accellion's unsecured FTA, Plaintiffs would not have done business with Impacted Clients or allowed their sensitive Personal Information to be entrusted to Accellion.

167. As a result of Accellion's violations of the UCL, Plaintiffs and Class Members are entitled to injunctive relief including, but not limited to: (1) ordering that Accellion cease support of the FTA platform; (2) ordering that Accellion utilize strong industry standard data security measures and file transfer software for the transfer and storage of customer data; (3) ordering that Accellion, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Accellion's systems on a periodic basis; (4) ordering that Accellion engage third party security auditors

and internal personnel to run automated security monitoring; (5) ordering that Accellion audit, test, and train security personnel regarding any new or modified procedures; (6) ordering that Accellion purge, delete, and destroy in a reasonably secure manner Class Member data not necessary for its provisions of services; (7) ordering that Accellion, consistent with industry standard practices, conduct regular database scanning and security checks; (8) ordering that Accellion, consistent with industry standard practices, evaluate all file transfer and other software, systems, or programs utilized for storage and transfer of sensitive Personal Information for vulnerabilities to prevent threats to customers and customers' customers; (9) ordering that Accellion, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (10) ordering Accellion to meaningfully educate its customers about the threats they face as a result of the loss of their Personal Information to third parties, as well as the steps Accellion's customers must take to protect themselves.

168. As a result of Accellion's violations of the UCL, Plaintiffs and Class Members have suffered injury in fact and lost money or property, as detailed herein. Class Members lost their Personal Information, which is their property, and privacy in that information. Class Members lost money as a result of dealing with the fallout of the Data Breach, including, among other things, negative credit reports, the value of time they expended monitoring their credit and transactions, resolving fraudulent charges, and resolving issues that resulted from the fraudulent charges and replacement of cards. Plaintiffs and Class Members are exposed to an ongoing risk of harm because their Personal Information is not adequately protected by Accellion, and is now in the hands of criminals. Plaintiffs and Class Members will continue to spend time, money, and resources in attempting to prevent and rectify fraud resulting from their Personal Information being exposed by Accellion.

169. Plaintiffs request that the Court issue sufficient equitable relief to restore them and Class Members to the position they would have been in had Accellion not engaged in violations of the UCL.

COUNT X
Declaratory Relief
28 U.S.C. § 2201
(On Behalf of Plaintiffs and the Class)

170. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

171. An actual controversy has arisen and exists between Plaintiffs and Class Members, on the one hand, and Accellion, on the other hand, concerning the Data Breach and Accellion's failure to protect Plaintiffs' and Class Members' Personal Information, including with respect to the issue of whether Accellion took adequate measures to protect that information. Plaintiffs and Class Members are entitled to judicial determination as to whether Defendant has performed and is adhering to all data privacy obligations as required by law or otherwise to protect Plaintiffs' and Class Members' Personal Information from unauthorized access, disclosure, and use.

172. A judicial determination of the rights and responsibilities of the parties regarding Defendant's privacy policies and whether Accellion failed to adequately protect Personal Information is necessary and appropriate to determine with certainty the rights of Plaintiffs and the Class Members, and so that there is clarity between the parties as to Accellion's data security obligations with respect to Personal Information going forward, in view of Accellion's continued custody of Personal Information.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of the Class, by and through undersigned counsel, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiffs as class representative and undersigned counsel as class counsel;

B. Award Plaintiffs and Class Members actual and statutory damages, punitive damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that Class Members have an effective remedy, including enjoining Accellion from continuing the unlawful practices as set forth above;

D. Award Plaintiffs and Class Members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiffs and Class Members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiffs and Class Members such other favorable relief as allowable under law or at equity.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: January 6, 2022

Respectfully submitted,

/s/ Tina Wolfson

TINA WOLFSON (SBN 174806)
twolfson@ahdootwolfson.com
ROBERT AHDOOT (SBN 172098)
rahdoot@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310.474.9111
Facsimile: 310.474.8585

ANDREW W. FERICH (admitted *pro hac vice*)
aferich@ahdootwolfson.com
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585

BEN BARNOW (admitted *pro hac vice*)
b.barnow@barnowlaw.com
ANTHONY L. PARKHILL (admitted *pro hac vice*)
aparkhill@barnowlaw.com
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Suite 1630
Chicago, IL 60606
Telephone: 312-621-2000
Facsimile: 312-641-5504

Attorneys for Plaintiffs and the Proposed Class